Remarks

The present amendment responds to the Official Action dated June 7, 2004. The Official Action rejected claims 1-15 under 35 U.S.C. 103(a) based on Nordman U.S. Patent No. 6,061,346 ("Nordman") in view of Bell U.S. Patent No. 6,707914 ("Bell"). This ground of rejection is addressed below following a brief discussion of the present invention to provide context. Claims 1, 7 and 10 have been amended to be more clear and distinct. Claims 1-15 are presently pending.

The Present Invention

Among its several aspects, a network according to the present invention includes a wireless network providing connectivity to client stations with improved security. Depending on design, the wireless network comprises one or more wireless access points connected to a central hub. The wireless network provides communication between the wireless access point or points and the client stations, but does not perform any authentication to control connection to the wireless access points. Any wireless client may obtain access to the wireless network through a wireless network access point.

A wireless network access point provides a connection to a Security Base (SB) server which controls access to the wired network by clients on the wireless network. The SB server has an interface with the wireless network, as well as an interface with the wired network. The SB server is typically connected to a network hub on the wired network and acts as a gateway to wired network resources for clients on the wireless network. When a wireless network client establishes a connection to the SB server, the SB server performs authentication for the wireless network client. Authentication is performed in order to verify that the wireless network client is authorized to gain access to the wired network. No authentication to the wireless network is required, and so the fact that a client has access to the wireless network does not imply that the client has any authorization for access to the wired network. Instead, control over the wired network is maintained by requiring each wireless network client to be authenticated as authorized to gain access to the wired network.

Once the wireless network client has been authenticated, the SB server provides the wireless network client with a temporary Internet protocol (IP) address on the wired network, using dynamic host control processing (DHCP). The SB server also provides the wireless network client with a unique session key to be used for encrypted communication with the wired network. The session key is used by one client during one connection session to the wired network.

The Art Rejections

All of the art rejections hinge on the application of Nordman and Bell, taken in combination. As addressed in greater detail below, the cited references do not support the Official Action's reading of them and the rejections based thereupon should be reconsidered and withdrawn. Further, the Applicant does not acquiesce in the analysis of the cited references made by the Official Action and respectfully traverses the Official Action's analysis underlying its rejections.

The Official Action rejected claims 1-15 under 35 U.S.C. 103(a) as unpatentable over Nordman in view of Bell. In light of the present amendments to claims 1, 7 and 10, this ground of rejection is respectfully traversed. In the discussion which follows below, the claims are discussed in the order as they were addressed by the Official Action.

Claim 10, as amended, claims establishing a connection between a wireless network access point and a security base (SB) server connected to a wired network. Claim 10 further claims establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point, exchanging encryption keys between the SB server and the wireless network client and transmitting authentication information from the wireless network client to the SB server through the wireless network access point. Claim 10 further claims performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network. If authentication fails, connection to the wired network is rejected. If authentication passes, connection to the wired network is accepted and a temporary wired network address and a unique session encryption key are provided to the wireless network client. Access is provided to wired network resources in response to requests by the wireless network client.

These limitations in the claimed combination are not taught by Nordman. Nordman teaches authentication of a wireless host in order to gain access to the wireless network. The wireless network establishes a connection to the IP network and provides a wireless host identifier, identifying the wireless host to the IP network. The wireless host is authorized to gain access to the IP network because the wireless host identifier is recognized as valid by the IP network, and because the wireless host has been authenticated by the wireless network for identification and access to the wireless network. Claim 10, by contrast, claims a wireless network client that is authenticated for access to a wired network without any need for access to the wireless network through which it gains a connection to the wired network. The wireless network is open to any user, but access to the wired network is controlled by the security base server, which receives and examines authentication information before allowing access to the wired network. Claim 10, as amended, therefore defines over Nordman.

Adding Bell to Nordman does not cure Nordman's deficiencies as a reference with respect to claim 10. Bell teaches providing a session key to an end station, but does not teach using a security base server connected to a wired network to authenticate a wireless network client as authorized to gain access to the wired network, as claimed by claim 10. Claim 10, as amended, therefore defines over the cited art and should be allowed.

Claim 1, as amended, claims a server connected to a wireless network access point and having access to a wired network. The server is operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point. The server performs authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network. The server is operative to establish a connection session upon authentication of a client, and is also operative to provide the client with a wired network address valid for the connection session upon authentication of the client, to encrypt communications with the wireless network access point and to provide a cryptographic key valid for the connection session to the client upon authentication of the client.

As noted above with respect to claim 10, neither Nordman, Bell, nor a combination thereof teaches or makes obvious a server operative to examine authentication information transmitted from the wireless network client to the server through a wireless network access point in order to determine if the wireless network client is authorized to gain access to the wired network. Claim 1, as amended, therefore defines over the cited art and should be allowed.

Claim 7, as amended, claims a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network. The wireless network access point is operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network. The wireless network access point is further operative to receive authentication information from one or more wireless network clients and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and determine if the information indicates that the wireless network client is authorized to access the wired network. The wireless network access point is further operative to receive a cryptoprocessing key from the server upon authentication of a client and to transfer the key to that client.

As noted above with respect to claim 10, neither Nordman, Bell, nor a combination thereof teaches or makes obvious a wireless access point receiving authentication information from a wireless network client and transferring the information to a server connected to a wired network in order to allow the server to examine the authentication information for the wireless network client and determine if the information indicates that the wireless network client is authorized to access the wired network. Claim 7, as amended, therefore defines over the cited art and should be allowed.

Conclusion

All of the presently pending claims, as amended, appearing to define over the applied references, withdrawal of the present rejection and prompt allowance are requested.

Respectfully submitted,

Peter H. Priest

Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713-7736
(919) 806-1600